

CERTIFIED COPY OF
PRIORITY DOCUMENT

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

#2
JC922 U.S. PTO
09/677968



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

1999年10月 7日

出 願 番 号
Application Number:

平成11年特許願第287262号

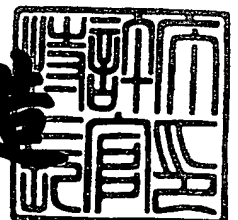
出 願 人
Applicant(s):

日本電気株式会社

2000年 8月 4日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3061098

【書類名】 特許願

【整理番号】 49230040

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/16

【発明者】

 【住所又は居所】 東京都港区芝五丁目 7 番 1 号
 日本電気株式会社内

 【氏名】 森本 伸一

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100082935

 【弁理士】

 【氏名又は名称】 京本 直樹

 【電話番号】 03-3454-1111

【選任した代理人】

 【識別番号】 100082924

 【弁理士】

 【氏名又は名称】 福田 修一

 【電話番号】 03-3454-1111

【選任した代理人】

 【識別番号】 100085268

 【弁理士】

 【氏名又は名称】 河合 信明

 【電話番号】 03-3454-1111

【手数料の表示】

 【予納台帳番号】 008279

 【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9115699

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 無線 LAN の暗号鍵更新システム及びその更新方法

【特許請求の範囲】

【請求項 1】

LAN 上に 1 以上の無線アクセスポイント装置 (AP) を有し、前記 AP は 1 以上の無線アクセス端末装置 (STA) と無線接続し、前記 STA との間でデータを暗号化して通信 (暗号化通信) する無線 LAN の暗号鍵更新システムにおいて、

前記 AP と LAN 接続された鍵管理サーバー装置 (SV) は前記 AP と前記 STA の暗号化通信に使用する k 個 (k は 1 以上) の暗号鍵を記憶する SV 記憶手段と、前記暗号鍵を生成し前記 SV 記憶手段に格納する暗号鍵生成手段とを有し、前記 SV は、前記 SV 暗号鍵生成手段にて前記暗号鍵を生成して前記 SV 記憶手段に格納し、予め設定された条件に従って前記暗号鍵生成手段を制御して前記 SV 記憶手段に記憶した前記暗号鍵を更新し、更新した前記暗号鍵を前記 AP と前記 STA に配信する、

ことを特徴とする、無線 LAN の暗号鍵更新システム。

【請求項 2】

前記 SV は、前記 SV 記憶手段に記憶された前記暗号鍵を更新する時、前記暗号鍵生成手段にて 1 時に暗号鍵を 1 個生成し更新する、

ことを特徴とする、請求項 1 に記載の無線 LAN の暗号鍵更新システム。

【請求項 3】

前記 SV は、前記 SV 記憶手段に記憶された前記暗号鍵を更新する時、前記暗号鍵生成手段にて 1 時に前記暗号鍵を 1 個生成し、前記 SV 記憶手段に記憶された k 個の暗号鍵を所定間隔で 1 個ずつ順次に更新する、

ことを特徴とする、請求項 1 に記載の無線 LAN の暗号鍵更新システム。

【請求項 4】

前記 SV は、前記 SV 記憶手段に記憶された k 個の前記暗号鍵の内、 $(k - 1)$ 個の暗号鍵については所定間隔 (間隔 1) で 1 個ずつ順次更新し、他の 1 個は $(k - 1)$ 個の暗号鍵より長い間隔 (間隔 2) で更新する、

ことを特徴とする、請求項 1 に記載の無線 LAN の暗号鍵更新システム。

【請求項 5】

前記 AP は、前記 SV の更新した第 n 番 (n は、 $1 \leq n \leq k$) の暗号鍵を配信されると前記 AP の記憶管理する第 n 番の暗号鍵を更新する手段と、第 n 番以外の暗号鍵を用いて暗号鍵更新通知伝文を暗号化して前記 STA に通知する手段とを有し、

前記 STA は、前記 AP から前記暗号鍵更新通知伝文を受けると STA 暗号鍵更新要求伝文を生成する手段と、前記暗号鍵更新通知伝文と同一の暗号鍵を用いて前記 STA 暗号鍵更新要求伝文を暗号化して前記 AP に通知する手段とを有し、

前記 AP は、さらに、前記 STA から前記 STA 暗号鍵更新要求伝文を受けると前記 SV へ STA 暗号鍵更新要求を通知する手段を有し、

前記 SV は、さらに、前記 AP から前記 STA 暗号鍵更新要求を受けると前記 STA 宛て暗号鍵配送の可否を判断する手段と、可と判断した場合に前記 AP へ前記 STA 宛て暗号鍵を配送する手段とを有する、

ことを特徴とする、請求項 2 乃至 4 の内、いずれか 1 に記載の無線 LAN の暗号鍵更新システム。

【請求項 6】

前記 AP は、前記 SV の更新した第 n 番 (n は、 $1 \leq n \leq k$) の暗号鍵を配信されると前記 AP の記憶管理する第 n 番の暗号鍵を更新する手段と、前記 AP の記憶管理する k 個の暗号鍵の内、最初に更新された暗号鍵を用いて暗号鍵更新通知伝文を暗号化して前記 STA に通知する手段とを有し、

前記 STA は、前記 AP から前記暗号鍵更新通知伝文を受けると STA 暗号鍵更新要求伝文を生成する手段と、前記暗号鍵更新通知伝文と同一の暗号鍵を用いて前記 STA 暗号鍵更新要求伝文を暗号化して前記 AP に通知する手段とを有し、

前記 AP は、さらに、前記 STA から前記 STA 暗号鍵更新要求伝文を受けると前記 SV へ STA 暗号鍵更新要求を通知する手段を有し、

前記 SV は、前記 AP から前記 STA 暗号鍵更新要求を受けると前記 STA 宛て暗号鍵配送の可否を判断する手段と、可と判断した場合に前記 AP へ前記 STA 宛て暗号鍵を配送する手段とを有する、

ことを特徴とする、請求項 2 乃至 4 の内、いずれか 1 に記載の無線 LAN の暗号鍵更新システム。

【請求項 7】

前記 AP は、さらに、前記 SV から前記 STA 宛て暗号鍵を配送されると STA 暗号鍵配送伝文を生成する手段と、第 n 番以外の暗号鍵を用いて前記 STA 暗号鍵配送伝文を暗号化して前記 STA に通知する手段とを有し、

前記 STA は、さらに、前記 AP から前記 STA 暗号鍵配送伝文にて第 n 番の暗号鍵を配送されると前記 STA の記憶管理する第 n 番の暗号鍵を更新する手段を有する、

ことを特徴とする、請求項 5、または 6 に記載の無線 LAN の暗号鍵更新システム。

【請求項 8】

前記 AP は、さらに、前記 SV から前記 STA 宛て暗号鍵を配送されると STA 暗号鍵配送伝文を生成する手段と、AP の記憶管理する k 個の暗号鍵の内、最初に更新された暗号鍵を用いて前記 STA 暗号鍵配送伝文を暗号化して前記 STA に通知する手段とを有し、

前記 STA は、さらに、前記 AP から前記 STA 暗号鍵配送伝文にて第 n 番の暗号鍵を配送されると前記 STA の記憶管理する第 n 番の暗号鍵を更新する手段を有する、

ことを特徴とする、請求項 5、または 6 に記載の無線 LAN の暗号鍵更新システム。

【請求項 9】

前記 STA は、所定の要因を検出すると、STA 暗号鍵一括更新要求伝文を AP へ通知する手段を有し、

前記 AP は、前記 STA から前記 STA 暗号鍵一括更新要求伝文を受けると前記 SV へ STA 暗号鍵一括更新要求を通知する手段を有し、

前記 SV は、前記 AP から前記 STA 暗号鍵一括更新要求を受けると前記 STA 宛て暗号鍵一括配送の可否を判断する手段と、可と判断した場合に前記 AP へ前記 STA 宛て暗号鍵を一括配送する手段とを有し、

前記 A P は、さらに、前記 S V から前記 S T A 宛て暗号鍵の一括配送を受けると S T A 暗号鍵一括配送伝文を生成して前記 S T A に通知する手段を有し、
前記 S T A は、さらに、前記 A P から前記 S T A 暗号鍵一括配送伝文を受けると前記 S T A の記憶する暗号鍵を一括して更新する手段を有する、
ことを特徴とする、請求項 1 乃至 4 の内、いずれか 1 に記載の無線 L A N の暗号鍵更新システム。

【請求項 1 0】

L A N 上に 1 以上の無線アクセスポイント装置 (A P) を有し、前記 A P は 1 以上の無線アクセス端末装置 (S T A) と無線接続し、前記 S T A との間でデータを暗号化して通信 (暗号化通信) する無線 L A N の暗号鍵更新方法において、
前記 A P と L A N 接続された鍵管理サーバー装置 (S V) は前記 A P と前記 S T A の暗号化通信に使用する k 個 (k は 1 以上) の暗号鍵を生成するとともに記憶管理し、予め設定された条件に従って更新し、更新した前記暗号鍵を前記 A P と前記 S T A に配信する、
ことを特徴とする、無線 L A N の暗号鍵更新方法。

【請求項 1 1】

前記 S V は、前記 S V の記憶管理する k 個の前記暗号鍵を更新する時、 k 個の暗号鍵の内、1 時に 1 個を更新する、
ことを特徴とする、請求項 1 0 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 2】

前記 S V は、前記 S V の記憶管理する k 個の前記暗号鍵を更新する時、 k 個の暗号鍵を所定間隔で 1 個ずつ順次に更新する、
ことを特徴とする、請求項 1 0 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 3】

前記 S V は、前記 S V の記憶管理する k 個の前記暗号鍵の内、 $(k - 1)$ 個の暗号鍵については所定間隔 (間隔 1) で 1 個ずつ順次に更新し、他の 1 個は $(k - 1)$ 個の暗号鍵より長い間隔 (間隔 2) で更新する、
ことを特徴とする、請求項 1 0 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 4】

前記 A P は、前記 A P の記憶管理する第 n 番 (n は、 $1 \leq n \leq k$) の暗号鍵を更新してから次に暗号鍵を更新するまでの間、前記 A P の記憶管理する第 n 番以外の任意の暗号鍵を用いて前記 S T A と暗号化通信する、
ことを特徴とする、請求項 1 1 乃至 1 3 の内、いずれか 1 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 5】

前記 A P は、前記 A P の記憶管理する第 n 番 (n は、 $1 \leq n \leq k$) の暗号鍵を更新してから次に暗号鍵を更新するまでの間、前記 A P の記憶管理する第 n 番以外の ($k - 1$) 個の暗号鍵を順次用いて前記 S T A と暗号化通信する、
ことを特徴とする、請求項 1 1 乃至 1 3 の内、いずれか 1 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 6】

前記 A P は、前記 A P の記憶管理する k 個の暗号鍵の内、最初に更新された暗号鍵を用いて前記 S T A と暗号化通信する、
ことを特徴とする、請求項 1 1 乃至 1 3 の内、いずれか 1 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 7】

前記 S T A は、前記 S T A の記憶管理する第 n 番以外の ($k - 1$) 個の暗号鍵の内、任意の暗号鍵を用いて前記 A P と暗号化通信する、
ことを特徴とする、請求項 1 4 乃至 1 6 の内いずれか 1 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 8】

前記 S T A は、前記 S T A の記憶管理する第 n 番以外の ($k - 1$) 個の暗号鍵を順次用いて前記 A P と通信する、
ことを特徴とする、請求項 1 4 乃至 1 6 の内いずれか 1 に記載の無線 L A N の暗号鍵更新方法。

【請求項 1 9】

前記 S T A は、前記 S T A の記憶管理する k 個の暗号鍵の内、最後に更新された暗号鍵を用いて前記 A P と通信する、

ことを特徴とする、請求項 1 4 乃至 1 6 の内いずれか 1 に記載の無線 LAN の暗号鍵更新方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、データを暗号化して無線通信する無線 LAN システムに関し、特に WEP メカニズムによる暗号化を用いた無線 LAN システムにおける暗号鍵更新システム及びその更新方法に関する。

【0 0 0 2】

【従来の技術】

従来、無線 LAN システムの普及に伴って、通信データの保護、すなわち、無線アクセスのセキュリティの確保が望まれていた。

【0 0 0 3】

近年、屋外用途だけでなく、屋内向けにも無線 LAN システムの導入が進んでいる。例えば、構内にアクセスポイント（AP：固定の基地局）を設置し、フロア内に設置する端末装置に送受信装置（STA）を接続して AP との間を無線化し、端末装置の配置変更の容易化、携帯型端末装置の帯出入に関する利便性向上を図るなどの例が増えている。

【0 0 0 4】

このようなシステムにおいては、例えば外来者の持ちこむ携帯型無線端末装置や、屋外へ漏洩する電波を傍受可能な外部の無線端末装置に対して、通信データを保護する必要がある。

【0 0 0 5】

無線通信におけるデータ保護の方式としては、暗号化を採用するものが一般化しつつある。無線データ通信における暗号化方式については、これまで IEEE で標準化の検討が進められてきた。

【0 0 0 6】

現在のところ、無線区間の暗号化及び認証の方式としては、IEEE 802.11 において、WEP（The Wired Equivalent Priv

acy algorithm) メカニズムを使用した、Shared Key 認証 (共通鍵) 方式が採用されている。

【0007】

図6 (a) は、IEEE 802. 11 の 8. 2. 3 章に記載されている、WE P メカニズムによる暗号化方式を示すブロック図、(b) は、同じく復号化方式を示すブロック図である。

【0008】

図6 (a) に示すように、WE P メカニズムによる暗号化方式は、Seed 生成手段 601、暗号化手段 602、誤り検出符号生成手段 603、誤り検出符号付加手段 604、及び暗号文生成演算手段 605 より構成され、暗号化メッセージ 606 を出力する。暗号化手段 602 は、RC4 アルゴリズムにより構成されている。

【0009】

図6 (a) の動作については IEEE 802. 11 ドラフト中に記載があるので説明を省略するが、図6 (a) の暗号化方式は、イニシャライゼーションベクタ (IV)、秘密鍵 (Secret Key)、及び通信データ (Plaintext) を入力し、IV と暗号文 (Ciphertext) を出力する。

【0010】

図6 (b) に示す、WE P メカニズムによる復号化方式は、Seed 生成手段 611、暗号化手段 612、復号化演算手段 613、符号分離手段 614、誤り検出符号生成手段 615、誤り検出符号比較手段 616 により構成されている。暗号化手段 612 は、RC4 アルゴリズムにより構成されている。

【0011】

図6 (b) の復号化方式は、受信した暗号化メッセージ 606 から IV と暗号文を入力し、復号方式側で予め設定され、記憶している秘密鍵を使用して復号演算処理を行う。この結果、復号した平文 (Plaintext) と、誤り検出符号 (ICV) 比較結果を出力する。

【0012】

図7 は、図6 (a) から (b) へ伝送される暗号化メッセージ 606 の構成を

示す。暗号化メッセージ606の構成は、拡張WEPフレームと称される。図7において各構成要素中に示す数字は、Octets（8ビット、以下「バイト」と記す）を単位としている。拡張WEPフレームは4バイトのIV701と、1バイト以上のデータ（PDU）702、4バイトのICV703により構成されている。拡張WEPフレームのデータ702、及びICV703は暗号化（Encrypt）され、IV701は暗号化されずに伝送される。

【0013】

IV701は、暗号化に使用する暗号鍵の識別情報を含んでいる。すなわち、図示する様に、IV701は3バイトのイニシャライズベクター本体704に、6ビットのパッド705と、2ビットの鍵ID（Key ID）706とからなる1バイトの情報707を付加して構成されている。

【0014】

この鍵ID706は2ビットの情報で構成されているので、4つまでの暗号鍵を識別することができる。従って、IEEE802.11の、WEPメカニズムを使用した暗号化方式においては、4つまでの暗号鍵を識別管理し、運用することができる。

【0015】

ところで、従来この種の無線通信に用いられる暗号化復号化技術、あるいは暗号通信装置としては、様々なものが提案されている。

【0016】

例えば、特開平11-196081号公報を参照すると、送信局と受信局とからなる暗号通信装置に適用できる暗号鍵の更新技術が開示されている。特開平11-196081号公報の発明によれば、暗号化によるデータ通信の手順は次のようである。

【0017】

すなわち、まず、送信側にて予備鍵を生成する。次に送信側にて暗号鍵を用いて暗号化した伝文により、予備鍵を送信する。送受信双方で予備鍵を暗号鍵として更新し、以降これを用いて暗号化、復号化を行い、データを通信する。

【0018】

この発明を実施するための構成の特徴としては、第 1 に予備鍵の記憶手段を有していること、第 2 に暗号鍵の記憶手段を有していること、第 3 に予備鍵を送信局が生成していることが挙げられる。

【0 0 1 9】

【発明が解決しようとする課題】

ところで、上記従来の暗号通信装置では、第 1 に鍵の管理を 1 対 1で行っている。このため、そのままでは 1 対多のシステムへの応用が難しいという問題を有していた。

【0 0 2 0】

また、多くの S T A と、A P との間で無線アクセス環境を提供するシステムへの応用を考えた場合、A P は、多くの端末のアクセスに使用する鍵を管理することとなる。例えば n 台の S T A を有するシステムでは、A P は n 台分の暗号鍵を記憶管理する手段が必要となるので、回路規模が増大するとともに、処理の負荷が増大するという問題を有していた。

【0 0 2 1】

また、可搬型の S T A を使用者が持ち運んで移動したり、フロアのレイアウト変更などによって S T A が移設されることによって、それまでとは異なる A P にアクセスすることとなった場合には、S T A と A P とで記憶管理している暗号鍵が不一致となり、通信できなくなるという問題を有していた。

【0 0 2 2】

さらに、特開平 1 1 - 1 9 6 0 8 1 号公報の発明を 1 対多のシステムへ応用することを考えた場合、A P は各 S T A に予備鍵を配送し、全ての S T A に予備鍵が行き渡った後、配布した予備鍵を暗号鍵として更新する手順が考えられる。しかしながら、このような手順で暗号鍵を更新しようとしても、全ての S T A が常時 A P にアクセスしているとは限らない状況においては、配送した予備鍵を暗号鍵に更新することができなくなる場合があるという問題を有していた。

【0 0 2 3】

従って、本発明の第 1 の目的は、多数の S T A と、A P の間で行われる暗号化通信システムに適用可能な暗号通信装置を提供することにある。

【 0 0 2 4 】

また、多数の S T A が A P と通信する暗号化通信システムにおいて、容易に暗号鍵を生成、管理可能な暗号通信方式を提供することを第 2 の目的とする。

【 0 0 2 5 】

また、可搬型の S T A を移動したり、S T A が移設されて、それまでとは異なる A P にアクセスすることとなった場合にも、新たな A P と、問題無くアクセスすることのできる暗号通信方式を提供することを第 3 の目的とする。

【 0 0 2 6 】

さらに、システムに属する全ての S T A が A P にアクセス可能な状態で無い場合にも随時暗号鍵を更新することで暗号化通信の信頼性を確保するとともに、暗号鍵の更新されなかった S T A に対する暗号鍵更新手順を設け、高い運用効率を有する暗号通信方式を提供することを第 4 の目的とする。

【 0 0 2 7 】

【課題を解決するための手段】

上記の目的を達成するため、本発明の暗号鍵更新方式は、1 以上の A P と L A N 接続された鍵管理サーバーを有し、全ての A P と S T A の間の暗号化無線通信に使用する暗号鍵を 1 組 (k 個) とし、一元的に管理するとともに、各 A P 、及び各 S T A に配送するよう構成している。

【 0 0 2 8 】

本発明の暗号鍵更新方式の A P は、k 個の暗号鍵記憶手段を有し、鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照して S T A と暗号化通信するよう構成している。

【 0 0 2 9 】

本発明の暗号鍵更新方式の S T A は、k 個の暗号鍵記憶手段を有し、A P 経由で鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照して A P と暗号化通信するよう構成している。

【 0 0 3 0 】

本発明の暗号鍵更新方式の S T A は、暗号鍵記憶手段に記憶された全ての暗号鍵が A P と一致しない場合、A P 経由で鍵管理サーバーに、暗号鍵の一括更新を

要求し、鍵管理サーバーから暗号鍵を一括配送されると S T A にて記憶管理していた暗号鍵を更新し、これを参照して A P と暗号化通信するよう構成している。

【 0 0 3 1 】

本発明の暗号鍵更新方法は、1 以上の A P と L A N 接続された鍵管理サーバーを有し、全ての A P と S T A の間の暗号化無線通信に使用する暗号鍵を 1 組 (k 個) とし、一元的に管理するとともに、各 A P 、及び各 S T A に配送する。

【 0 0 3 2 】

本発明の暗号鍵更新方法の A P は、k 個の暗号鍵記憶手段を有し、鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照して S T A と暗号化通信する。

【 0 0 3 3 】

本発明の暗号鍵更新方法の S T A は、k 個の暗号鍵記憶手段を有し、A P 経由で鍵管理サーバーから配送される暗号鍵を記憶管理し、これを参照して A P と暗号化通信する。

【 0 0 3 4 】

本発明の暗号鍵更新方法の S T A は、暗号鍵記憶手段に記憶された全ての暗号鍵が A P と一致しない場合、A P 経由で鍵管理サーバーに、暗号鍵の一括更新を要求し、鍵管理サーバーから暗号鍵を一括配送されると S T A にて記憶管理していた暗号鍵を更新し、これを参照して A P と暗号化通信する。

【 0 0 3 5 】

【発明の実施の形態】

以下に、本発明の実施の形態について、図面を参照して説明する。

【 0 0 3 6 】

図 1 は本発明の実施の形態による無線 L A N システムの構成を示すブロック図である。図 1 に示す、本発明による無線 L A N システムは、鍵管理サーバー 1 0 1 、A P 1 0 2 、複数 (m 台) の A P (# 1 S T A 1 0 3 - 1 、# 2 S T A 1 0 3 - 2 、… # m S T A 1 0 3 - m) より構成されている。

【 0 0 3 7 】

A P 1 0 2 と S T A 1 0 3 との間は I E E E 8 0 2 . 1 1 による無線 (W i r

e l e s s) L A N接続にて構成されている。

【0038】

STAとAPとの間のデータ通信では、WEPメカニズムを使用した暗号化方式を用いる。WEPメカニズムを使用した暗号化方式では、STAとAPは、それぞれ4個の暗号鍵を記憶管理し、暗号化、復号化を行う。

【0039】

図1の鍵管理サーバー101は、AP102とSTA103との間の無線区間において、暗号化に使用する暗号鍵を生成、管理する。鍵管理サーバーは新たな鍵を生成すると、AP102、STA103へ配送する。

【0040】

AP102は、鍵管理サーバー101から暗号鍵を配送されると、STA103との通信に使用する暗号鍵を更新し、記憶管理するとともに、STA103に暗号鍵の更新を通知する。

【0041】

STA103は、鍵管理サーバー101からAP102を経由して配送された暗号鍵を記憶管理し、暗号鍵を使用してAPと通信する。

【0042】

図2は、AP102の構成を示すブロック図である。図2に示す、本発明によるAP102は、制御手段201、暗号鍵設定手段202、第1鍵記憶手段203、第2鍵記憶手段204、第3鍵記憶手段205、第4鍵記憶手段206、鍵選択手段207、鍵ID生成手段208、IV生成手段209、平文入力手段210、WEP暗号化手段211、暗号文送出手段212、暗号文入力手段213、WEP復号手段214、平文出力手段215、及び、鍵ID抽出手段216より構成されている。

【0043】

ここで、WEP暗号化手段211は、図6(a)にて説明した、IEEE802.11のWEPによる暗号化方式にて構成されている。また、WEP復号化手段214は、図6(b)にて説明したIEEE802.11のWEPによる復号化方式にて構成される。

【0044】

図2に示す、第1乃至第4の鍵記憶手段203乃至206は、図1にも示すように、MIBと称されるバッファにより構成することができる。MIBはソフトウェアによって書換えることは可能であるが、ソフトウェアによって読み出すことは不可能な構造を持つ、情報秘匿性の高い記憶手段である。

【0045】

尚、図2に示す暗号鍵生成手段200は、鍵管理サーバーに含まれる。

【0046】

図3は、STA103の構成を示すブロック図である。図3に示す、本発明によるSTA103は、制御手段301、暗号鍵設定手段302、第1鍵記憶手段303、第2鍵記憶手段304、第3鍵記憶手段305、第4鍵記憶手段306、鍵選択手段307、鍵ID生成手段308、IV生成手段309、平文入力手段310、WEP暗号化手段311、暗号文送出手段312、暗号文入力手段313、WEP復号化手段314、平文出力手段315、及び、鍵ID抽出手段316より構成されている。図3に示す、第1乃至第4の鍵記憶手段303乃至306は、図2に示した鍵記憶手段と同様、MIBにより構成することができる。

【0047】

図4、図5は、本発明による無線LANシステムにおける、暗号鍵の更新手順を示すシーケンスチャートである。

【0048】

図4は、通常の暗号鍵更新手順を示している。すなわち、STAとAPは、互いに同じ暗号鍵を記憶管理している状態で、鍵管理サーバーが新たな暗号鍵を生成した場合に、AP、及びSTAに配送し、更新する場合の手順である。

【0049】

図5は、STAとAPとで記憶管理している暗号鍵が4個とも一致しない状態で、STAの記憶管理する暗号鍵を更新する場合の手順を示す。すなわち、例えば、携帯型のSTA装置を長期に渡って帯出し、AP側の暗号鍵が全て更新された後に帯入してAPにアクセスしようとした場合、或いは、あるSTAが長期に渡って稼動されることなく放置され、AP側の暗号鍵が全て更新された後に稼動

された場合などに適用する、暗号鍵更新手順である。

【0050】

まず、通常の暗号鍵更新の動作について、図4、及び図1乃至図3を参照して説明する。

【0051】

図4において鍵管理サーバーは、4個の暗号鍵うち任意の1個（ n 番）を新たに生成し、鍵管理サーバー内に記憶管理している第 n 番目の暗号鍵を更新する（ n 番の鍵更新）と、APに配送（AP鍵配送）する。

【0052】

APは鍵管理サーバーからAP鍵配送を受けると、AP内に記憶管理している4個の内、第 n 番目の暗号鍵を更新（ n 番の鍵更新）し、STAに対して鍵の更新を通知（鍵更新通知）する。この時、APからSTAへ送信される鍵更新通知には、暗号鍵は含まれていない。ただ、APは第 n 番以外の暗号鍵を用いて、鍵更新通知伝文を暗号化する。

【0053】

ここで、鍵管理サーバーからAPへ配送された暗号鍵の鍵IDが1（ $n=1$ ）であるとして、図2を参照して説明する。

【0054】

図2を参照すると、鍵管理サーバーの有する暗号鍵生成手段200は、新たに暗号鍵を生成すると、APの制御手段201へ配送（AP鍵配送）する。APの制御手段201は、鍵管理サーバーから配送された暗号鍵と、鍵ID（1）を暗号鍵設定手段202へ転送する。暗号鍵設定手段202は、制御手段から受け取った暗号鍵を、鍵IDに対応して第1鍵記憶手段203に格納し、更新する。

【0055】

次に制御手段201は、平文入力手段210と鍵ID生成手段208とを制御して、STAへ鍵の更新を通知する。平文入力手段210は、制御手段からの制御により、鍵更新通知伝文を生成し、WEP暗号化手段211に入力する。鍵ID生成手段208は、更新された鍵のIDとは違うIDを生成する。ここでは、例として鍵ID「2」を出力するものとする。鍵選択手段207は、第2鍵記憶

手段 2 0 4 に記憶されている暗号鍵を選択し、W E P 暗号化手段 2 1 1 に入力する。I V 生成手段 2 0 9 は、鍵 I D を 2 とした I V を生成し、W E P 暗号化手段 2 1 1 に入力する。

【 0 0 5 6 】

W E P 暗号化手段 2 1 1 は、I V 生成手段 2 0 9 から入力された I V と、鍵選択手段 2 0 7 から入力された暗号鍵を使用して平文入力手段 2 1 0 から入力される鍵更新通知伝文を暗号化する。暗号文出力手段 2 1 2 は、W E P 暗号化手段 2 1 1 の作成した暗号文と I V を入力し、拡張 W E P フレームを構成して送信装置などに出力する。

【 0 0 5 7 】

図 4 に戻り、S T A は、A P から鍵更新通知を受けると、A P 経由で鍵管理サーバー宛てに鍵の更新を要求する。これを受けて、鍵サーバーは S T A の真正性をチェックし、S T A 鍵配送可と判断すると、A P 経由で S T A 宛てに暗号鍵を配送する。S T A は、鍵管理サーバーから S T A 鍵配送を受けると、新たな暗号鍵を記憶管理する。

【 0 0 5 8 】

本発明による無線 L A N システムにおいては、S T A と A P 間の無線区間に以上の手順を採用することによって、より高い安全性を確保している。

【 0 0 5 9 】

S T A が鍵更新通知を受け、鍵の更新を要求する動作について、図 3 を参照して説明する。

【 0 0 6 0 】

図 3 を参照すると、A P からの鍵更新通知は、暗号文入力手段 3 1 3 に入力され、I V と暗号文に分けられて復号化手段 3 1 4 に入力される。W E P 復号化手段 3 1 4 は、入力される I V を鍵 I D 抽出手段 3 1 6 へ出力する。鍵 I D 抽出手段 3 1 6 は、I V 中の鍵 I D を取り出して鍵選択手段 3 0 7 を制御する。

【 0 0 6 1 】

図 2 の動作説明で I V の鍵 I D は「2」としたので、鍵選択手段 3 0 7 は第 2 鍵記憶手段 3 0 4 を選択する。W E P 復号化手段 3 1 4 は、鍵選択手段 3 0 7 の

出力する第2鍵を入力されて、鍵変更通知伝文を復号処理する。平文出力手段315は、WEP復号化手段314の復号した平文を出力する。

【0062】

制御手段301は、平文出力手段315の出力を参照し、鍵更新通知を検出すると、鍵更新要求伝文を返送する。制御手段301は、鍵ID抽出手段316の出力する鍵IDを参照し、鍵ID生成手段308へ転送する。鍵ID生成手段308は、制御手段から受け取った鍵ID「2」を出力する。鍵選択手段307はこれにより第2鍵記憶手段を選択する。IV生成手段309は、鍵ID「2」のIVを生成する。また、制御手段301は、平文入力手段310を制御して鍵更新要求伝文を生成する。

【0063】

WEP暗号化手段311は、IV生成手段309から入力されたIVと、鍵選択手段307から入力された暗号鍵を使用して平文入力手段310から入力される鍵更新要求伝文を暗号化する。暗号文出力手段312は、WEP暗号化手段311の作成した暗号文とIVを入力し、拡張WEPフレームを構成して送信装置などに出力する。

【0064】

次に、STAから鍵更新要求を受けたAPが、鍵管理サーバーへ鍵更新要求伝文を送出し、鍵管理サーバーからのSTA鍵配送をSTAへ送出手続きについて、図2を参照して説明する。

【0065】

図2において、STAからの鍵更新要求伝文は、暗号文入力手段213に入力され、IVと暗号文に分けられて復号化手段214に入力される。WEP復号化手段214は、入力されるIVを鍵ID抽出手段216へ出力する。鍵ID抽出手段216は、IV中の鍵IDを取り出して鍵選択手段207を制御する。

【0066】

STAの送出手続きしたIVの鍵IDは「2」であるので、鍵選択手段207は第2鍵記憶手段204を選択する。WEP復号手段214は、鍵選択手段207の出力する第2鍵を入力されて、鍵変更要求伝文を復号処理する。平文出力手段21

5は、WEP復号化手段214の復号した平文を出力する。

【0067】

制御手段201は、平文出力手段215の出力を参照し、鍵更新要求を検出すると、鍵管理サーバーへ鍵更新要求伝文を送出する。

【0068】

STAの出力する鍵更新要求伝文には、STA固有の情報を含み、鍵管理サーバーにて鍵配送の可否判断のため、参照される。すなわち、STAは、固有の情報として、STAのMACアドレス、STA使用者の識別情報、パスワードなどを鍵更新要求伝文に含めて送出手する。

【0069】

鍵管理サーバーはこれらSTAからの固有情報と、予め各STAに関して登録された固有情報とを比較する。そして、受け取った鍵更新要求伝文の送出元STAの真正性が確認された場合に限り、STA宛てに暗号鍵を配送する。

【0070】

図2を参照すると、鍵管理サーバーの有する暗号鍵生成手段200は、STA宛ての暗号鍵をAPの制御手段201へ配送（STA鍵配送）する。APの制御手段201は、鍵管理サーバーから配送されたSTA鍵配送伝文を、平文入力手段210に入力する。次に鍵ID生成手段208を制御して、STAへ暗号鍵を配送する。平文入力手段210は、制御手段からのSTA鍵配送伝文を、WEP暗号化手段211に入力する。鍵ID生成手段208は、鍵ID「2」を出力する。鍵選択手段207は、第2鍵記憶手段204に記憶されている暗号鍵を選択し、WEP暗号化手段211に入力する。IV生成手段209は、鍵IDを2としたIVを生成し、WEP暗号化手段211に入力する。

【0071】

WEP暗号化手段211は、IV生成手段209から入力されたIVと、鍵選択手段207から入力された暗号鍵を使用して平文入力手段210から入力されるSTA鍵配送伝文を暗号化する。暗号文出力手段212は、WEP暗号化手段211の作成した暗号文とIVを入力し、拡張WEPフレームを構成して送信装置などに入力する。

【0072】

続いて、STAがSTA鍵配送伝文を受け、暗号鍵を更新する動作について、図3を参照して説明する。

【0073】

図3を参照すると、APからのSTA鍵配送伝文は、暗号文入力手段313に入力され、IVと暗号文に分けられて復号化手段314に入力される。WEP復号化手段314は、入力されるIVを鍵ID抽出手段316へ出力する。鍵ID抽出手段316は、IV中の鍵IDを取り出して鍵選択手段307を制御する。

【0074】

鍵選択手段307は鍵IDに従って、第2鍵記憶手段304を選択する。WEP復号化手段314は、鍵選択手段307の出力する第2鍵を入力されて、STA鍵配送伝文を復号処理する。平文出力手段315は、WEP復号化手段314の復号した平文を出力する。

【0075】

制御手段301は、平文出力手段315の出力を参照し、STA鍵配送伝文を検出すると、受け取ったSTA鍵を暗号鍵設定手段302に転送する。暗号鍵設定手段302は、受け取った平文に含まれる、配送された暗号鍵のIDを参照して、対応する鍵記憶手段に格納し、暗号鍵を更新する。この例では、第1鍵を更新するので、平文には鍵ID「1」が含まれる。従って、新たな暗号鍵は第1鍵記憶手段303に格納される。

【0076】

以上説明した動作によって、鍵管理サーバーの生成する暗号鍵をAP、及びSTA宛てに配送し、それぞれの記憶管理する暗号鍵を更新することができる。

【0077】

次に、多数のSTA、及び、複数のAPに対する、暗号鍵の管理について説明する。

【0078】

本発明の無線LANシステムでは、鍵管理サーバーに複数のAPが接続される場合がある。そして、システムに係属するSTAは、フロアレイアウトの変更、

または、可搬型STAの移動によって、それまでとは別のAPにアクセスする場合も考えられる。これらの条件に鑑み、複数のAPに加え、多数のSTAの暗号鍵を容易に管理可能とするため、本発明の無線LANシステムにおいては、鍵管理サーバーは、各AP、STAに配送する暗号鍵を、システム全体に渡って共通の1組（4個）としている。こうすることによって、管理する暗号鍵の数を最小限に留めてシステムの負荷を低減することができる。また、複数のAPに渡ってSTAを移動した場合にも、各APが同一の暗号鍵を有するので、暗号鍵不一致の発生を回避することができる。

【0079】

次に、本発明の無線LANシステムにおける、暗号鍵の更新、及びSTAとAPにおける暗号鍵の運用について説明する。

【0080】

IEEE 802.11のWEPでは、4個の暗号鍵を識別して管理、運用することができる。そこで、本発明の無線LANシステムでは、4個の暗号鍵の更新、及び、APとSTAとがそれぞれ通信する場合の暗号鍵の運用について、次に示す幾つかの方法を採用し、高い運用性と情報秘匿性の両立を図っている。

【0081】

暗号鍵更新方法の第1として、鍵管理サーバーは、4個の暗号鍵をある一定の期間が経過するごとに、1個ずつ順次更新していく。具体的には、1週間経過する毎に、1個ずつ順次更新する。こうすることによって、それぞれの暗号鍵は4週間に1度、更新されることとなる。従って、携帯型のSTAを帯出する者は、4週間以内にSTAを帯入すれば、問題無くAPにアクセスすることができる。

【0082】

この期間の長さは、鍵管理サーバーにて設定可能としてもよく、システムの要求によって、例えば1日毎、1ヶ月毎などとしてもよい。

【0083】

この要領で暗号鍵を更新するシステムでは、STAとAPは次に示す、幾つかの方法で暗号鍵を運用する。

【0084】

その 1 によれば、AP は 4 個の暗号鍵の内、最後に更新した暗号鍵を通信に使用せず、他の 3 個を順次用いて STA と通信する。

【0085】

複数の STA が存在するシステムにおいては、全ての STA の記憶管理する暗号鍵の更新には時間を要する。すなわち、暗号鍵の更新は鍵管理サーバーから AP、STA に対して個別に行われるため、AP が暗号鍵を 1 個更新した時、各 STA は AP からの暗号鍵更新通知を受けて逐次鍵管理サーバーへ暗号鍵更新要求を行い、鍵管理サーバーから鍵配送を受けて個々に暗号鍵を更新する。

【0086】

この方法を採用することによって、AP が 1 個の暗号鍵を更新してから、全ての STA の記憶管理する暗号鍵の更新が完了するまでの間、暗号鍵の不一致に起因する障害を回避することが可能となる。

【0087】

その 2 によれば、AP は、最初に更新した暗号鍵を用いて STA と通信する。

【0088】

こうすることによって、STA はより長い期間に渡って暗号鍵更新の機会を得ることができる。

【0089】

上記第 1 の暗号鍵の更新方法における、その 1、及びその 2 の暗号鍵の使用方法において、STA は、STA の記憶管理する暗号鍵の内、最後に更新されたものを使用して通信する。こうすることによって、携帯型 STA の帯出可能期間、あるいは STA の非稼動可能期間を最も長くすることができる。尚、情報秘匿性向上のために、最後に更新された暗号鍵以外の暗号鍵を適宜利用してもよい。

【0090】

暗号鍵更新方法の第 2 として、鍵管理サーバーは、特定の暗号鍵の更新周期を他の暗号鍵の更新周期よりも大幅に長く設定し、他の暗号鍵はより短い更新周期で順次更新する。具体的には、第 1 の暗号鍵は 3 ヶ月毎に更新し、第 2 乃至第 4 の鍵については、1 日毎に 1 個ずつ順次更新する。こうすることによって、携帯型の STA を帯出する者は、3 ヶ月以内に STA を帯入すれば、問題無く AP に

アクセスすることができるので、利便性が向上するとともに、他の 3 個の暗号鍵は 3 日周期で更新されるため、これを通信に利用すれば情報秘匿性は向上する。

【 0 0 9 1 】

尚、この方法においても、暗号更新周期は、システムの要求によって、任意に定められてよいことは、云うまでも無い。

【 0 0 9 2 】

この要領で暗号鍵を更新するシステムでは、S T A と A P は次に示す、幾つかの方法で暗号鍵を使用することができる。

【 0 0 9 3 】

その 1 によれば、A P は 3 日周期で更新される暗号鍵を適宜使用して、S T A と通信する。A P と一致した暗号鍵を記憶管理している S T A も、3 日周期で更新される暗号鍵を使用して通信することで、S T A と A P 間の通信における情報の秘匿性は高く保つことができる。しかしながら、S T A が 3 日以上帯出された後、帯入されて A P にアクセスする場合、あるいは、3 日以上非稼動状態にあった S T A が再度稼動されて A P にアクセスする場合には、暗号鍵の不一致を生じる。この場合 A P は、その 2 に示す方法により、S T A と通信する。

【 0 0 9 4 】

その 2 によれば、A P は S T A からの伝文の暗号鍵が、A P にて記憶管理するものと不一致を生じた場合、3 ヶ月周期で更新する暗号鍵を用いて S T A との通信を試みる。この方法で暗号鍵が一致した場合、A P は S T A に対して暗号鍵の更新を通知する。S T A はこれにより暗号鍵更新要求を行い、鍵管理サーバーから最新の暗号鍵を配送され、更新することができる。

【 0 0 9 5 】

ところで、上記第 2 の暗号鍵更新方法を用いても、3 ヶ月を超えて長期に渡る S T A の帯出、あるいは非稼動に対しては、全ての暗号鍵が不一致となる。

【 0 0 9 6 】

次に、このような場合の暗号鍵更新動作について、図 5 を参照して説明する。

【 0 0 9 7 】

図 5 を参照すると、A P と一致する暗号鍵を有しない S T A は、例えば第 1 鍵

から順次 S T A にて記憶管理している暗号鍵を使用して、A P にアクセスを要求（アクセス要求 1 回目）する。A P は、暗号鍵が一致しないので、平文を使用して鍵の不一致を通知（鍵 N G 通知 1 回目）する。

【 0 0 9 8 】

暗号鍵の不一致を 4 回繰り返すと、S T A は平文を利用して、鍵の一括更新を要求（鍵の一括更新要求）する。A P は、S T A からの鍵の一括更新要求を鍵管理サーバーへ転送する。このとき、暗号鍵の一括更新要求伝文には、S T A の個別情報が含まれることは、図 4 にて説明した動作と同様である。

【 0 0 9 9 】

鍵管理サーバーは S T A の個別情報をチェックし、真正性を確認すると、A P 経由で S T A 暗号鍵を一括して配送する。S T A は鍵管理サーバーからの S T A 暗号鍵一括配送を受けると、記憶管理していた暗号鍵を一括して更新する。

【 0 1 0 0 】

次に S T A は、新たな暗号鍵を使用して A P にアクセスを要求する。A P は暗号鍵を確認し、一致すると、通常の日タ通信を開始する。

【 0 1 0 1 】

尚、図 5 は、理解の容易のため S T A は 4 回に渡ってアクセス要求するものとしているが、より効率的なシーケンスも考えられることは云うまでも無い。すなわち、S T A は 4 個の暗号鍵の内、最後に更新された暗号鍵を第 1 回目のアクセス要求に使用し、これが不一致となった場合には、直ちに鍵の一括更新を要求する、などのシーケンスが考えられる。

【 0 1 0 2 】

ところで、図 5 のシーケンスチャートにおいて、S T A の暗号鍵一括更新要求から S T A 暗号鍵一括配送までの、S T A と A P 間の無線通信は、平文で行うものとしている。これは、図 5 は、A P と S T A の間の無線区間を含む、別途の暗号化通信を適用することを前提としているためである。

【 0 1 0 3 】

すなわち、図 5 上部に示すように、鍵管理サーバーから S T A までの区間において、あるいは、A P から S T A までの区間において、公開鍵を使用するなどに

より、本発明とは別途の暗号化復号化を併用することで、図 5 のシーケンスにおいて安全に S T A の暗号鍵を更新することが可能となる。

【0 1 0 4】

本発明によれば、S T A の記憶管理する 4 個の暗号鍵の全てが A P と一致しない状態となっても、無線 L A N システムによって暗号鍵を一括更新する（すなわち、人間系によって暗号鍵を S T A に設定するなどの作業を介さずに暗号鍵を更新可能とする）ことができる。

【0 1 0 5】

【発明の効果】

以上説明したように本発明によれば、1 以上の A P と L A N で接続された鍵管理サーバー装置を有し、全ての A P と S T A の間の暗号化無線通信に使用する暗号鍵を 1 組（k 個）とし、鍵管理サーバー装置にて一元的に管理することによって、暗号鍵の管理のために装置の回路規模が増大することもなく、また、暗号鍵の管理のために処理の負荷が増大することもなく、容易に 1 対多の無線 L A N システムを提供することができる。

【0 1 0 6】

また、本は発明によれば、可搬型の S T A を使用者が持ち運んで移動したり、フロアのレイアウト変更などによって S T A が移設されることによって、それまでとは異なる A P にアクセスすることとなった場合にも、S T A と、S T A のアクセスする A P との間で記憶管理している暗号鍵が不一致となることがない、無線 L A N システムを提供することができる。

【0 1 0 7】

さらに、本発明によれば、可搬型の S T A を使用者が長期に帯出したために S T A の暗号鍵の更新がされず、再度帯入した時には S T A の記憶していた全ての暗号鍵が、アクセスした A P と不一致する状態となった場合にも、S T A に対する暗号鍵の更新手順を提供するので、人間系の操作による煩雑な対応処置を必要とせずに S T A の記憶していた暗号鍵を更新できる、高い運用性を有する暗号通信方式を提供することができる。

【図面の簡単な説明】

【図 1】

本発明の無線 LAN システムの構成を示すブロック図である。

【図 2】

本発明の AP の構成を示すブロック図である。

【図 3】

本発明の STA の構成を示すブロック図である。

【図 4】

本発明の暗号鍵更新手順を説明するためのシーケンスチャートである。

【図 5】

本発明の暗号鍵更新手順を説明するためのシーケンスチャートである。

【図 6】

従来の技術において、IEEE 802. 11 の WEP による暗号化方式を説明するためのブロック図である。

【図 7】

従来の技術において、IEEE 802. 11 の WEP による復号化方式を説明するためのブロック図である。

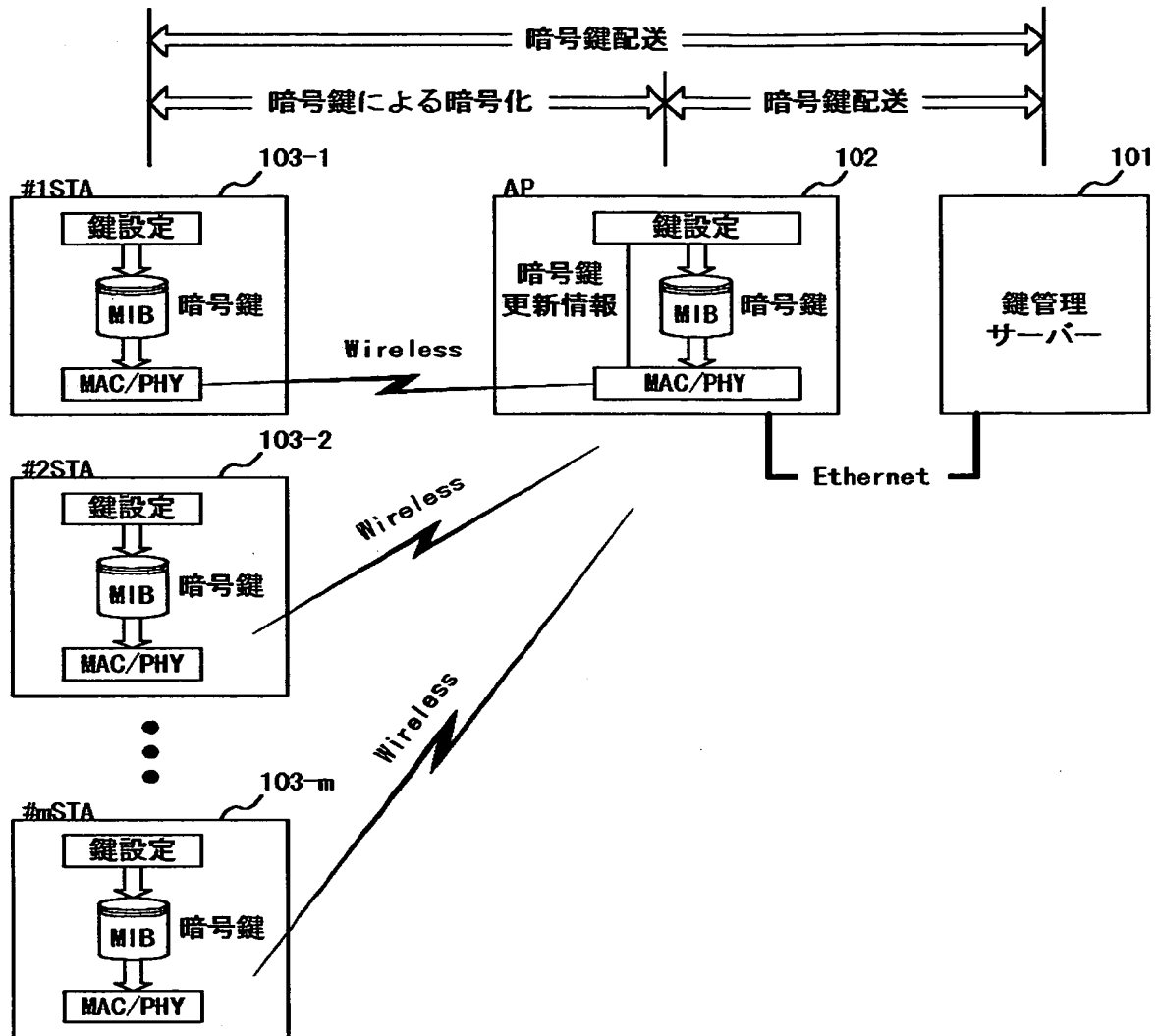
【符号の説明】

- 1 0 1 鍵管理サーバー
- 1 0 2 AP
- 1 0 3 STA
- 2 0 0 暗号鍵生成手段
- 2 0 1 制御手段
- 2 0 2 暗号鍵設定手段
- 2 0 3 第 1 鍵記憶手段
- 2 0 4 第 2 鍵記憶手段
- 2 0 5 第 3 鍵記憶手段
- 2 0 6 第 4 鍵記憶手段
- 2 0 7 鍵選択手段
- 2 0 8 鍵 ID 生成手段

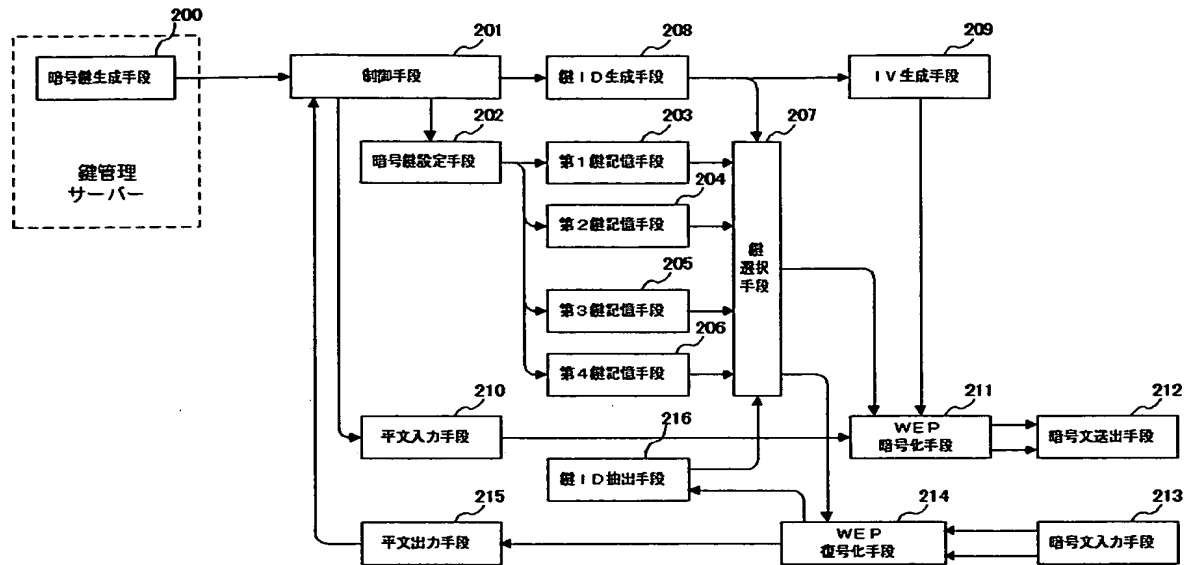
- 2 0 9 I V 生成手段
- 2 1 0 平文入力手段
- 2 1 1 W E P 暗号化手段
- 2 1 2 暗号文送出手段
- 2 1 3 暗号文入力手段
- 2 1 4 W E P 復号化手段
- 2 1 5 平文出力手段
- 2 1 6 鍵 I D 抽出手段
- 3 0 1 制御手段
- 3 0 2 暗号鍵設定手段
- 3 0 3 第 1 鍵記憶手段
- 3 0 4 第 2 鍵記憶手段
- 3 0 5 第 3 鍵記憶手段
- 3 0 6 第 4 鍵記憶手段
- 3 0 7 鍵選択手段
- 3 0 8 鍵 I D 生成手段
- 3 0 9 I V 生成手段
- 3 1 0 平文入力手段
- 3 1 1 W E P 暗号化手段
- 3 1 2 暗号文送出手段
- 3 1 3 暗号文入力手段
- 3 1 4 W E P 復号化手段
- 3 1 5 平文出力手段
- 3 1 6 鍵 I D 抽出手段

【書類名】 図面

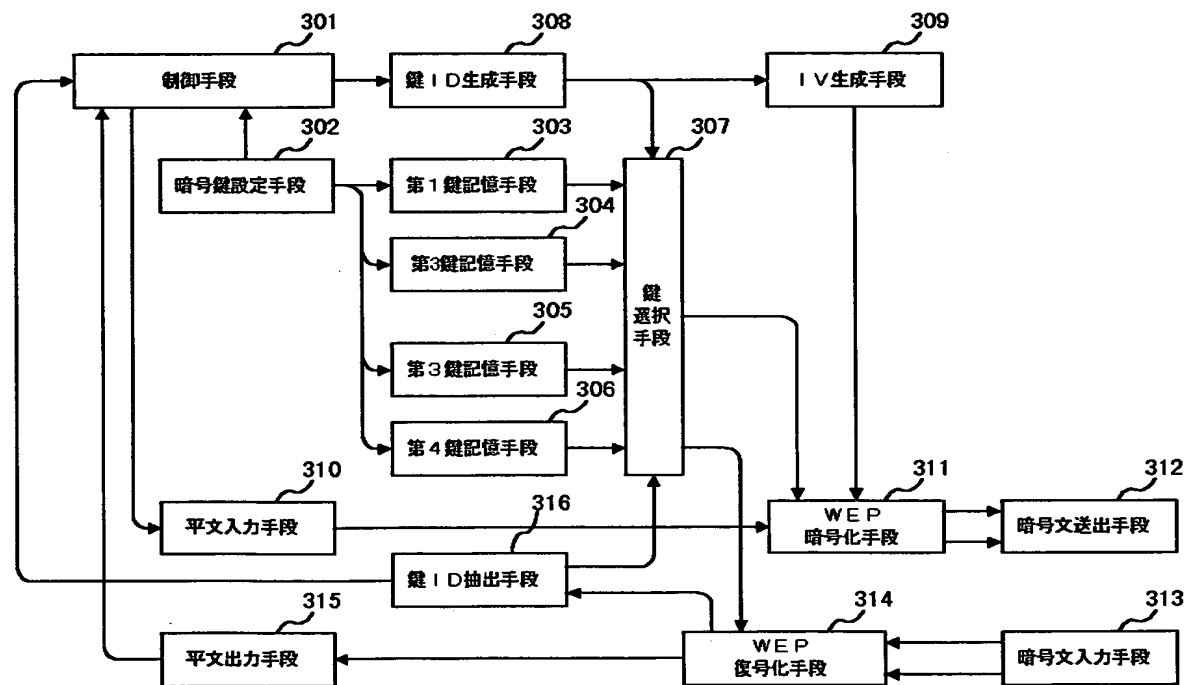
【図 1】



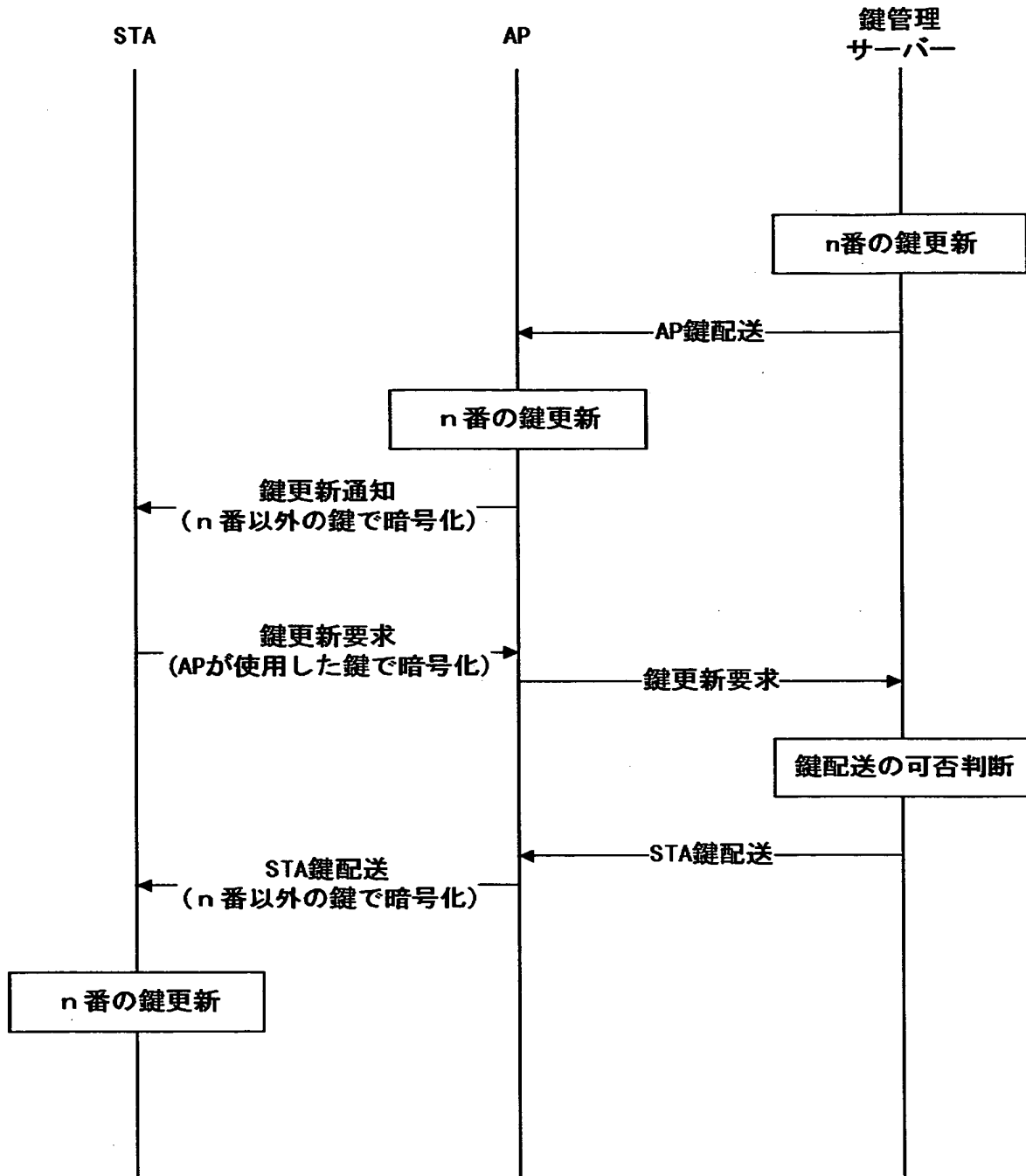
【図 2】



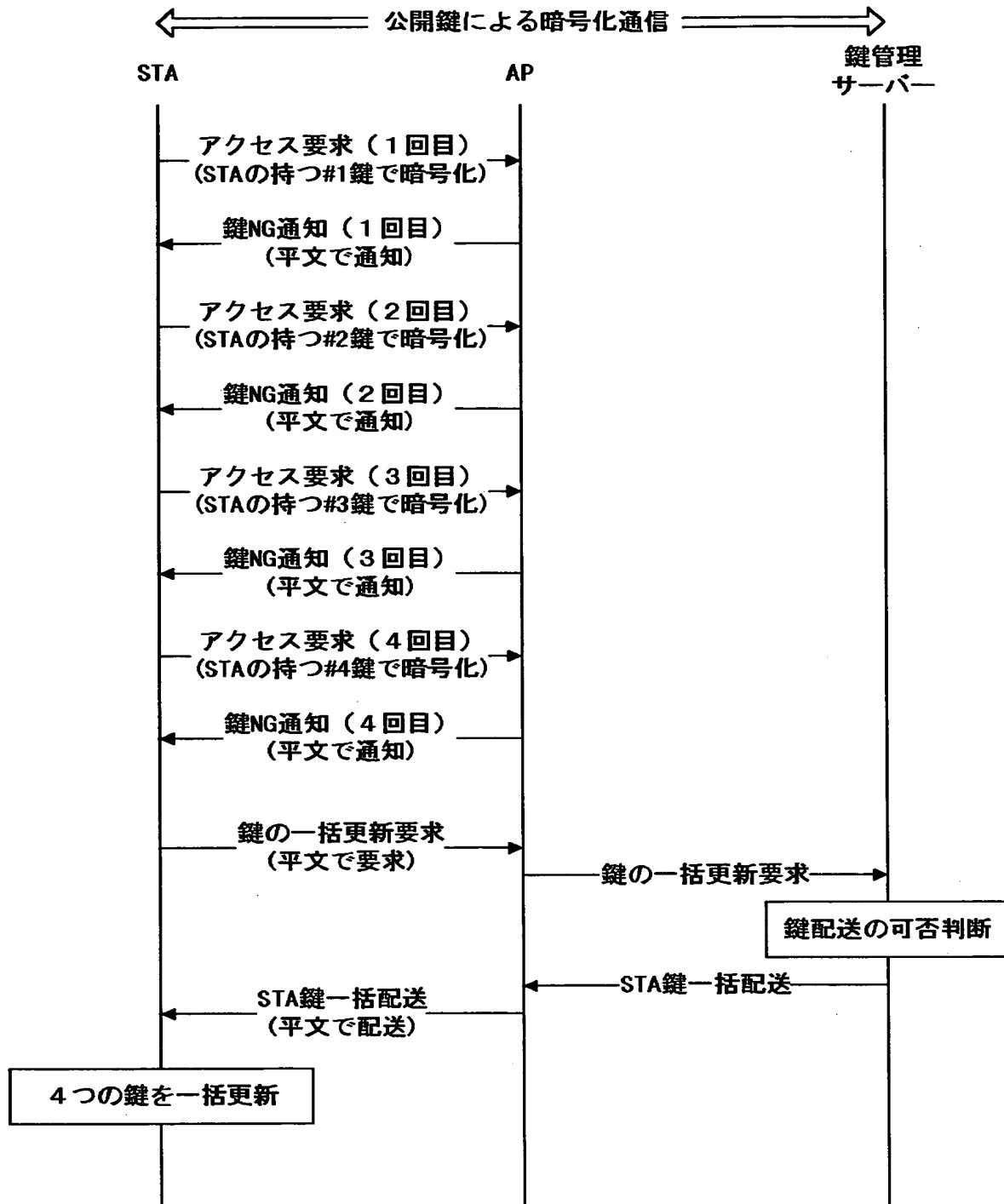
【図 3】



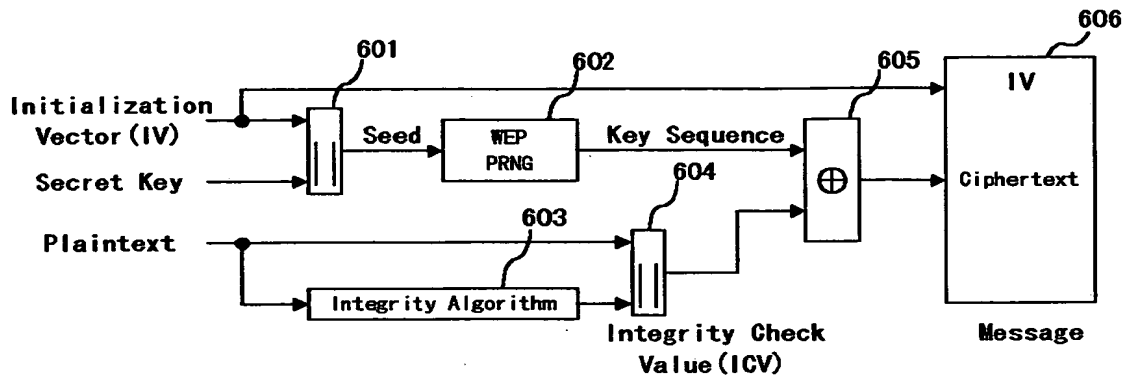
【図 4】



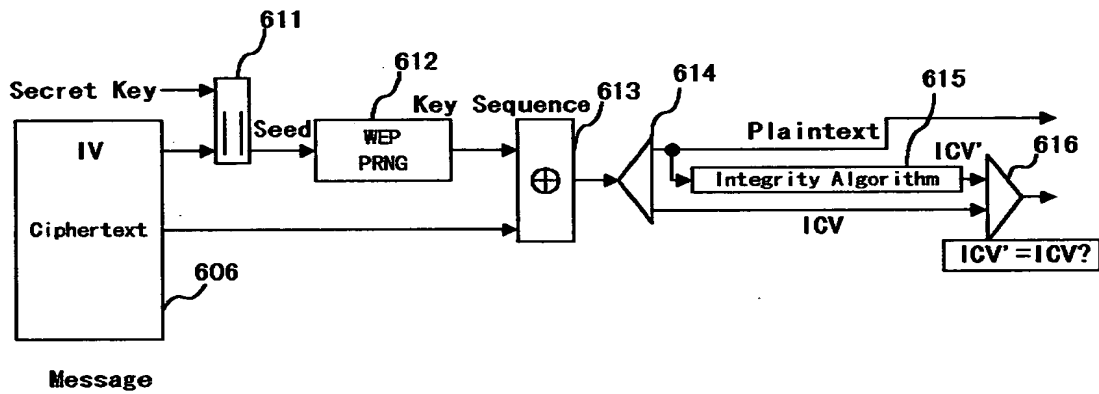
【図 5】



【図 6】

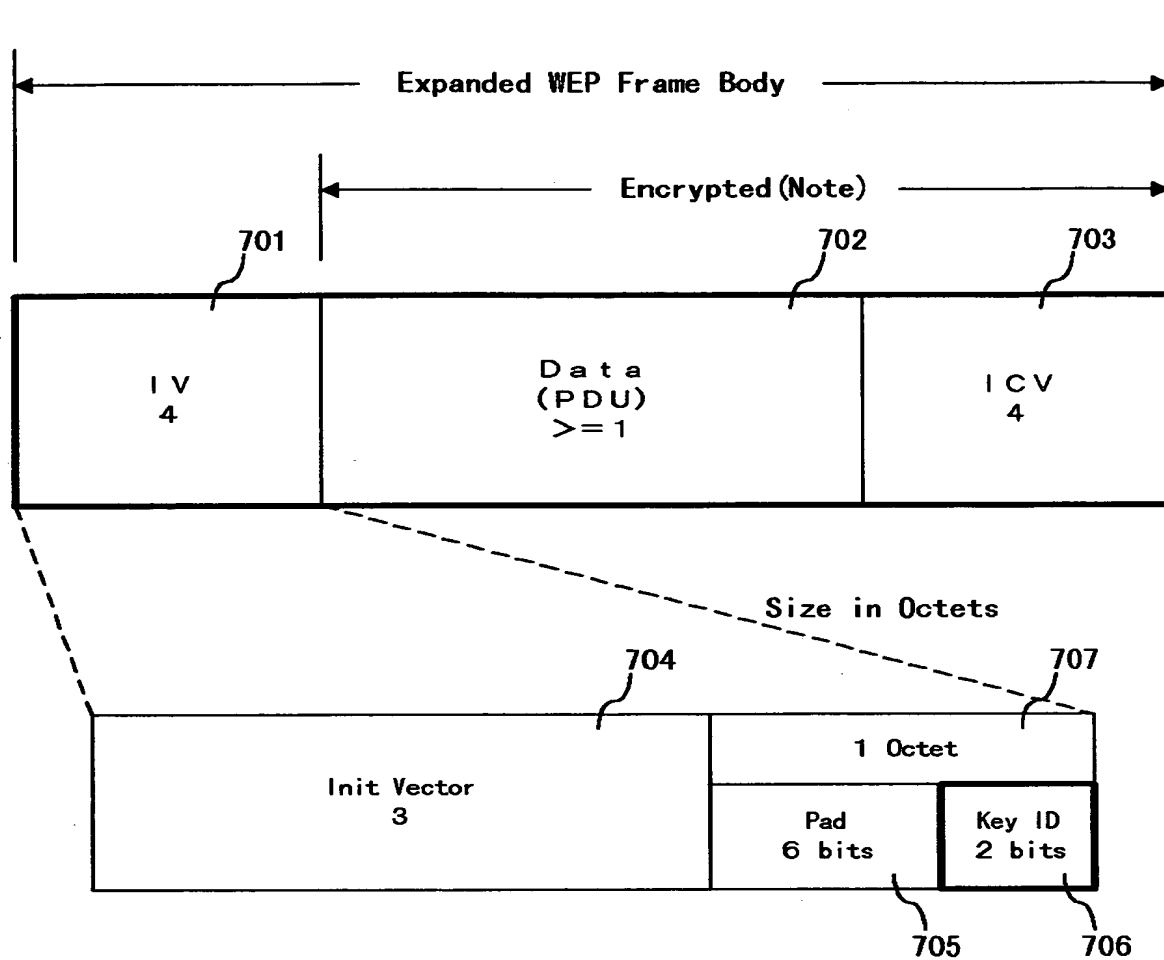


(a)



(b)

【図 7】



【書類名】 要約書

【要約】

【課題】 複数のＡＰ、多数のＳＴＡを有する無線ＬＡＮシステムに、ＩＥＥＥ 8 0 2．1 1のＷＥＰを適用できる、暗号鍵更新方式及び更新方法を提供する。

【解決手段】 ＡＰとＬＡＮ接続された鍵管理サーバーを有し、全てのＡＰとＳＴＡの間の暗号化無線通信に使用する暗号鍵を１組（ｋ個）とし、一元管理するとともに、鍵管理サーバーにて暗号鍵を更新すると、各ＡＰ、及び各ＳＴＡに配送するよう構成している。

【選択図】 図 1

認 定 ・ 付 加 情 報

特許出願の番号	平成 1 1 年 特許願 第 2 8 7 2 6 2 号
受付番号	5 9 9 0 0 9 8 6 5 1 6
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 1 年 1 0 月 1 2 日

< 認定情報・付加情報 >

【提出日】	平成11年10月 7日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 2 3 7]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[変更理由]	新規登録
住 所	東京都港区芝五丁目 7 番 1 号
氏 名	日本電気株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.